Performance Study of Black Hole Attack Detection Technique using AODV in MANET

Ranjan Bishnoi

Research Scholar, Department of Information Technology,
G.B. Pant University of Agriculture & Technology,
Pant Nagar-263145 UK INDIA
ranjanbishnoi2602@gmail.com

Hardwari Lal Mandoria

Professor and Head, Department of Information Technology,
G.B. Pant University of Agriculture & Technology,
Pant Nagar-263145 UK INDIA
drmandoria@gmail.com

ABSTRACT

A mobile ad hoc network is aninfrastructure lessnetwork where mobile nodes position themselves in anabrupt fashion or most of the time communication takes place while nodes are moving. Such networks are also featured by dynamic topology i.e. the topology changes from time to time. Because of autonomous nature and dynamic behavior of MANET any node from external environment can add itself to the network and behave maliciously leading to various commonly known attacks e.g. flooding attacks, link withholding attack, link spoofing attack, replay attack, wormhole attack , colluding misrelay attack etc.One such attack is a Black Hole Attack .This paper aims at studying the impact of such an attack for AODV protocol on the network performances considered in terms of various performance metrics as throughput, end to end delay and packet delivery ratio.The simulation is carried out in network simulator2 (ns2). At last a probability based solution is proposed to detect and counter the effect of black hole attack to the noticeable extent.

Keywords*:* MANET, AODV, Black hole attack**.**

I. INTRODUCTION

A MANET is an autonomous collection of mobile users that communicate over wireless links.

Because of the mobile nature of nodes, the network topology changesrapidly with time. Nodes can communicate with each other directly only if they are within the radio range and when they are not, communication takes place using multi hop routing.[19][20]

During communication nodes continuously move into and out of the radio range causing certain breakage in transmission or incomplete or improper transmission is there.

As compared to the wired network, MANET is more vulnerable to the attacks caused by any node that behaves maliciously within the network. So first we study the following features make MANET vulnerable to attacks.

- *Absenceof a centralized node*:Due to the lack of centralized node detection of attacks become difficult because there is no one tomonitor the traffic in a highly dynamic and large scale adhocnetwork[10].
- *Topology being dynamic*: Timely changing topology disturbs the trustful communication among nodes. The trust may also be disturbed if some nodes are detected as compromised i.e. the node within the network behaves maliciously [14].
- *Power supply is limited*: A node in mobile ad-hoc network may behave in a selfish manner if it finds out that there is only limited power supply [18][29].
- *Bandwidth limitation*: Low capacity links exists in MANET as compared to wireless network to provide hindrance against external noise, interference and signalattenuation effects [17][28].
- *Changing Scalability*: The scalability is also dynamic in such networks as nodes are mobile and move randomly so the security mechanism implied should be applicable for both small scale and large scale ad-hoc networks.[30]
- *Autonomous System*: .The nodes work in a free environmentwhere they are allowed to join and leave the wirelessnetwork at any point of time. This is the main vulnerability issue.[23][24][25]

In our study, we have chosen AODV protocol because of its wide usage and vulnerability to attacks. The main reason for it being most vulnerable protocol is its underlying mechanism.Simulations are carried out using ns-2 (Network Simulator version 2. Firstly tests on different topologies to compare the network performance with and without black holes in the network were taken.The presence of a black hole node made sure that the performance deteriorated.

We also proposed a probability based solution that reduces the effect of black hole attack and leads to a better network performance.

Our study is categorized into different sections: section II discusses the AODV protocol and its underlying mechanism. In Section III we have discussed the black hole attack and the works of various authors and their approach towards detecting the black hole. Section IV covers the different simulation parameters. In section V, the simulation results have been discussed. Section VI covers the conclusion part.

II. AD-HOC ON DEMAND DISTANCE VECTOR PROTOCOL (AODV):

AODV is a reactive routing protocol vulnerable to black hole attacks. If a node has to start transmission with another node in the network to which it has no route, AODV will provide topology information for the node. Control messages are used to find a route to the destination node in the network. There are three types of control messages in AODV which are discussed below. :

A. Route Request Message (RREQ):

When a source node needs to communicate with another node in the network it transmits RREQ message. AODV uses flooding for RREQ message. There is a time to live (TTL) value in every RREQ message, where the value of TTL states the number of hops the RREQ should be transmitted through.

B. Route Reply Message (RREP):

A Route reply (RREP) meansa node having a requested identity or any intermediate node that has a route to the requested node generates a route reply(RREP) message back to the source node.

C. Route Error Message (RERR):

Every node in the network keeps monitoring the link status to its neighbor's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

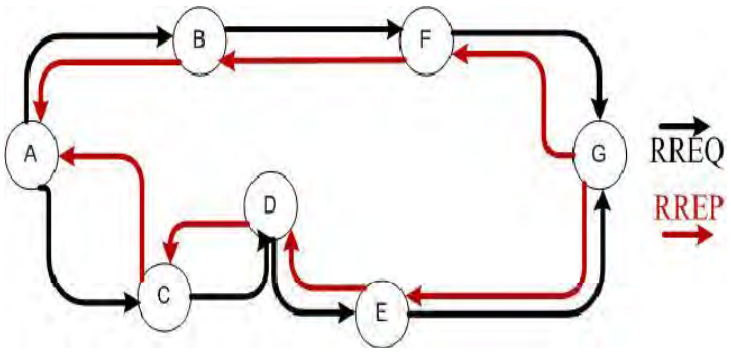

Fig. 1: Route Discovery in AODV [21][22]

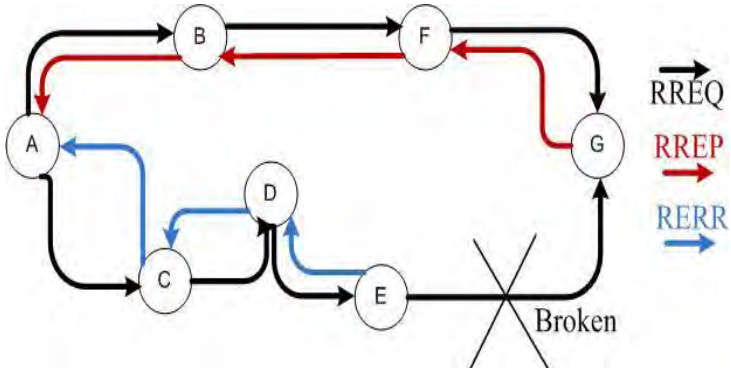

Fig. 2: Route Error Message in AODV[21][22]

In AODV, sequence numbers are used in the RREP messages. Sequence numbers act as time stamps that allow nodes to compare how fresh their information on the other node is. When a node sends any type of routing control message RREQ, RREP, RERR etc., it increases its own sequence number. If the sequence number is higher it is assumed to be more accurate information and the node that sends the highest sequence number, route is established over this node by the other nodes.

III. BLACKHOLE ATTACK

In black hole attack, a malicious node either compromised or external, advertises itself as having the shortest path to the destination node. The attacker node advertises availability of fresh routes to the other nodes without even checking its routing table [26]. This is how an attacker node indicates the route availability as reply to the route request messages and thus capture the data packet and retain it. In flooding based protocol requesting node receives the malicious node reply before the reception of reply from actual node and therefore a forged route is created. After this route is established,the node drops all the packets.

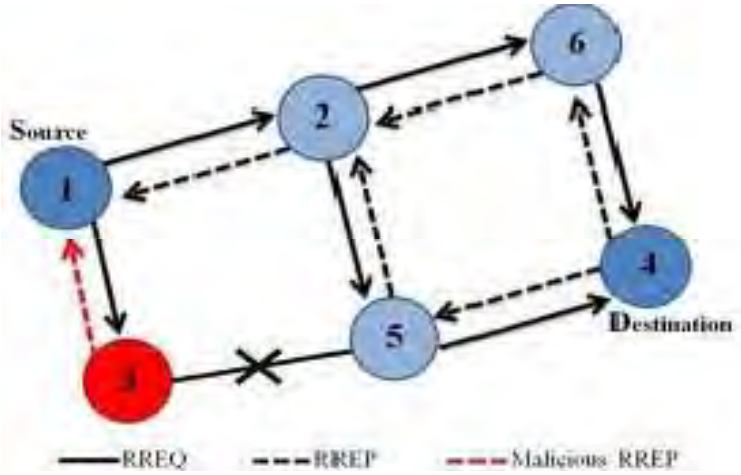

Fig. 3: Black hole attack [27]

A mobile ad-hoc network is very much vulnerable to the black hole attack. This was the major concern of various authors who studied and proposed different solutions against the black hole attack.

Hesiri Weerasinghe et al. [2] proposed a solution to identify and prevent the cooperative black hole attack. Solution discovers the secure route between source and destination by identifying and isolating cooperative black hole nodes. Evaluation of the proposed solution and comparison with other existing solutions in terms of throughput, packet loss percentage, average end-to-end delay and route request overhead is done. Their experiments show that the AODV greatly suffers from cooperative black holes in terms of throughput and packet losses, and solution proposed presents good performance in terms of better throughput rate and minimum packet loss percentage over other solutions, and that it can accurately prevent the cooperative black hole attacks.

Latha Tamilselvan et al. [3]havealso givenan approach to combat the Black hole attack. One of the principal routing protocols used in Ad hoc networks is AODV (Ad hoc on demand Distance Vector) protocol. The security of the AODV protocol is compromised by a particular type of attack called 'Black Hole' attack.

Soufine Djahel etal. [4] proposed "An Acknowledgment - Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol". The paper aims at investigating the effects of the cooperative black hole attack against OLSR, in which two colluding MPR nodes cooperate in order to disrupt the topology discovery is done. Then an Acknowledgment based technique is proposed that overcomes the shortcomings of the OLSR protocol, and makes it less vulnerable to such attacks by identifying and then isolating malicious nodes in the network. The simulation results of the proposed scheme show high detection rate under various scenarios.

Htoo Maung Nyo et al. [5]performed a work wherethey have shown simulation results by using individual reputation system, alert on finding a black hole node and exchanging neighbor information messages on meeting a new neighbor will help detecting and eliminating malicious or black hole nodes from the networks.

M. Khalili shoja et al. [6] proposed awork in whichthe effect of black hole attack on ad hoc networks is investigated.Furthermore, hash chain is used to prevent this type of attack in a network that uses AODV as a routing protocol and results of applying this method has been investigated. Simulation resultsusing OPNET simulator indicates that packet delivery ratio, in the presence of malicious nodes, reduces remarkably and proposed approach can prevent the effect of black hole attacks.

Yingbin Liang et al. [7] have investigated the secrecy throughput of mobile ad hoc networks (MANETs) with malicious nodes. A model under active attack is further studied, in which the malicious nodes actively attack the network by transmitting modified packets to the destination nodes. It is shown that to guarantee the same throughput as the model under passive attack, the model under active attack needs to satisfy more stringent condition on the number of malicious nodes.

Rajib Das et al. [8] have given an algorithmic approach to focus on analyzing and improving the security of AODV, which is one of the popular routing protocols for MANET. Presented aim is on ensuring the security against Black hole attack.

Monita Wahengbamet al. [9] implemented a fuzzy rule to detect the misbehavior over the network. The work will analyze the traffic over a node and take a fuzzy decision regarding the node reliability. The parameters in paper are number of successful data transmitted over the node, number of packets lost.

IV. SIMULATION

In our study ,we have used Network Simulator (Version 2.35).It is widely known as NS2 and is an event driven simulation tool that has is useful for studying the dynamic nature of communication networks[12][13].Simulation of wireless, wired network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviors.

A. Network performance parameters

Following network performance metrics are usedto analyze the simulation results:

1. Packet delivery ratio (PDR): It is the ratio total number of packets received to the total no. of packets sent. Results also get affected by the inclusion of the routing packets

   $$PDR = \Sigma \text{ Number of packets received} / \Sigma \text{ Number of packet send} \quad (1)$$

2. End-to-end Delay (E2E Delay): It is the average time taken by a packet to travel from source to destination.The parameter gets affected by the increase in the number of intermediate mobile nodes.

   $$E2E\ Delay = \Sigma \text{ (arrived time} - \text{send time)} / \Sigma \text{ Number of connections} \quad (2)$$

3. Throughput: It is defined as the successful data transmitted per unit time.The parameter varies directly with the number of packets received and is inversely proportional to the end to end delay.Thus, these two are the deciding factors for the throughput.

   $$Throughput = \Sigma received\ packets\ /(arrived\ time\text{-}send\ time)*2000*8/1000\ in\ kbps. \quad (3)$$

   Here, “2000” indicates the packet size we have taken for the simulationand the time taken is in seconds.
4. Number of Packets received: Other parameter we have taken into consideration is the number of packets received. This acts as the unit for all the other parameters[11][15][16].

B. Simulation Parameters

In this section, we describe the various parameters we have considered for our simulation .The value options chosen for the simulation depends on various factors including size of the network, the number of connections ,the method of transmission etc.

The Simulation environment parameters considered for our simulation are defined in the following table.

TABLE 1: SIMULATION PARAMETERS

PARAMETERS	VALUES
Simulation Area Size	750 x750,1500 x 1500
Number of nodes	10,20,30,40
Interface queue type	Queue/ DropTail / PriQueue
MAC protocol	IEEE 802.11
Radio range of a node	100m
Traffic Type	CBR
Transport Layer Protocol	UDP
Network Layer Protocol	AODV/ blackholeAODV/ IdAODV
Simulation Time	400 s
Queue length	50
Packet Size	2000 bytes
mobility model	Antenna/OmniAntenna

V. DISCUSSION OF SIMULATION RESULTS

We have considered two scenarios for comparison.

In our first scenario,an environment with a blackhole node is considered and our other environment gives result of our proposed work.For our comparison,we have considered the performance factors discussed in Section V. The graphs plotted show a detailed comparison between the two scenarios.

Here the first line (dashed blue line) represents the blackhole node environment (blackholeAODV)and the second one (double line compound red) represents the one with blackhole but with intrusion detection mechanism(idAODV).

Simulation results are shown as follows:

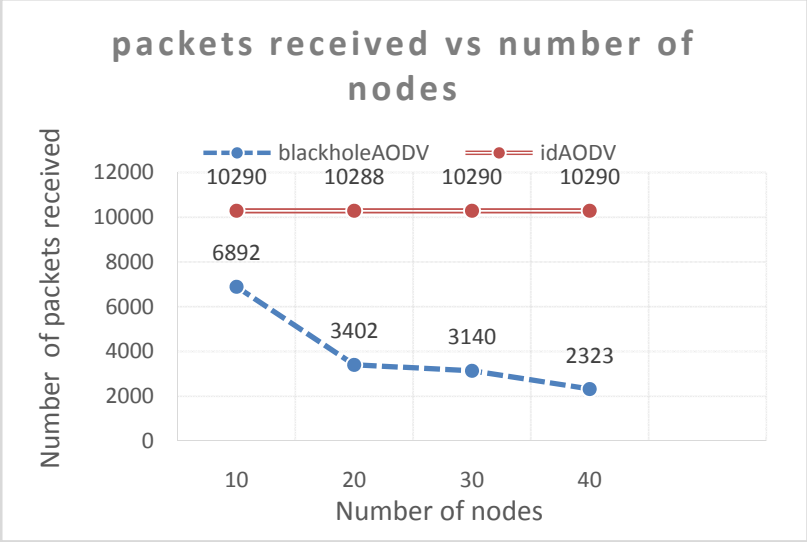

Fig. 4: Number of packets received

In Fig.4, we have shown the change in the number of packets received at the destination with the change in the number of nodes. In case of Black Hole Attack scenario, the reason behind the decrement in the number of

packets received with the increase in number of nodeslies in the fact that in addition to the black hole node ,we also have the more number of mobile intermediate nodes which may or may not be able to forward the packets to the destination due to various reasons e.g. multiple transfers ,queue length exceeds or others .However in case of our solution i.e. the one with the solution, we get a nearly ideal results as only those control packets are dropped that lie beyond threshold. These are generally three or four in numbers.

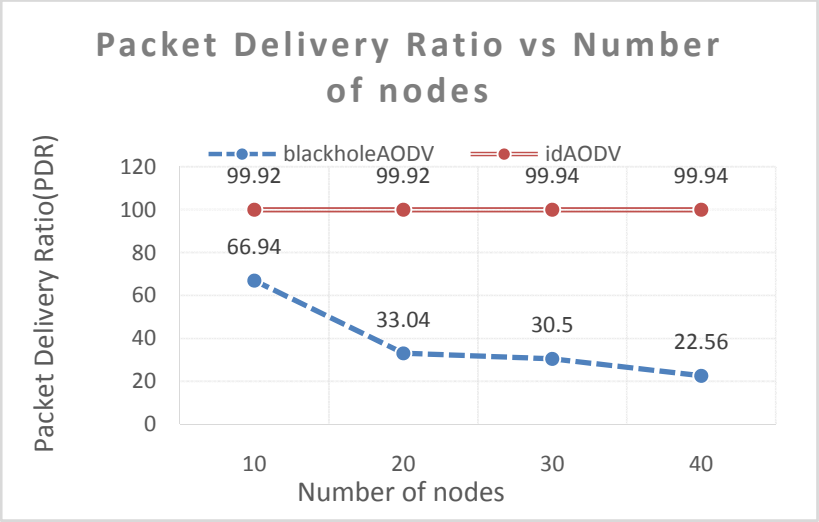

Fig. 5: Packet Delivery Ratio (PDR)

Fig. 5 depicts the change in PDR with the change in number of nodes.In case of Black Hole Attack scenario, the same reason can be accounted for the fall of PDR with the increase in number of nodes as was provided for the number of packet received with the number of nodes. Now since the number of packets sent remain the same but the number of packets received decreases, according to eq. (1) from section IV, the PDR decreases gradually. However, in case of the scenario with our solution provided, the ideal number of packets received ensure that PDR value doesn't drop and remains consistent.

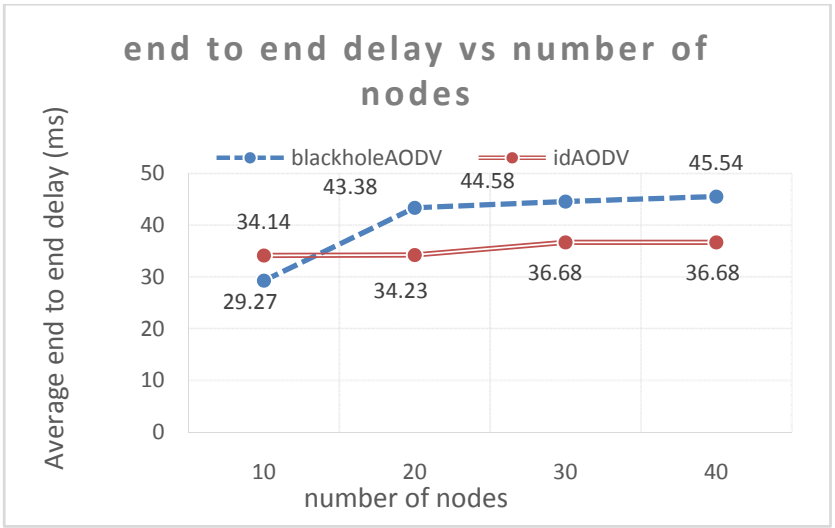

Fig. 6: Average End to End Delay (E2E Delay)

In Fig. 6, we have shown the effect of change in number of nodes on Average end to end delay. Now in case of both our scenarios, the one with Black Hole Attack and the one with solution provided, we can observe that as the number of nodes in the network increases, the E2E Delay also increases. This increased delay is introduced by the increase in the number of intermediate mobile nodes. As, for e.g. if there could be associated a single intermediate node for packet to reach the destination, now there are many to increase the transfer time of each packet and thereby the E2E Delay.

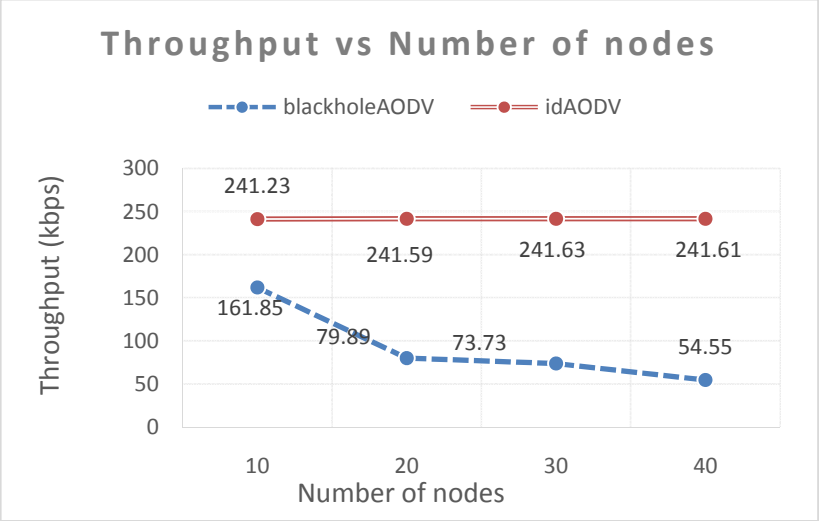

Fig. 7: Throughput

Fig. 7 shows the change in the throughput with the change in number of nodes. As can be observed from eq. (3) of section IV, throughput varies inversely w.r.t. end to end delay. Thus, the decrease in Throughput is fairly reasonable in case of a Black Hole Attack scenario but in case of our solution since the increase in Average end to end delay is hardly noticeable, so is the case with the throughput. The given explanation holds, if only considered that number of packets received remains same, which is true in most of the cases we have taken. So the inverse relation with Average end to end delay is far dominant than the direct one with number of packets received.

VI. CONCLUSION

From the study ,we finally conclude that the probability based algorithm provides a significant approach towards a black hole free network environment without any overhead for using a separate procedure to detect a black hole node and then for preventing it. It only uses the deductions from previous works and a probability based solution to provide some eye catching results. A significant improvement in all the parameters can be observed, be it a PDR, E2E Delay or Throughput.

The step is just one little step towards a bigger scenario. The algorithm can be used as a submodule in other approaches towards black hole detection or prevention and also can be extended to the study of cooperative blackhole attack i.e. where more than one node act as blackholes. Also it can be used as generalized approach in other routing protocols such as Dynamic Source Routing (DSR).

REFERENCES

[1] Elmar Gerhards-Padilla," Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", 32nd IEEE Conference on Local Computer Networks 0742-1303/07, 2007
[2] Hesiri Weerasinghe and Huirong Fu "Preventing Cooperative Black hole Attacks in Mobile Ad hoc Networks", International Journal of Software Engineering and its Applications, Vol. 2, No. 3, pp. 39-54, 2008.
[3] Latha Tamilselvan "Prevention of Co-operative Black Hole Attack in MANET" International journal of networks, vol. 3, no. 5, May 2008.
[4] Soufine Djahel , Farid Na¨ıt-Abdesselam and Ashfaq Khokha"An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" , Proc. of IEEE Beijing, 2008.
[5] Htoo Maung Nyo and Piboonlit Viriyaphol "Detecting and Eliminating Black Hole in AODV Routing", IEEE International Conference on Communication (ICC) 2009.
[6] M. Khalili, H. Taheri, S. Vakilinia, "Preventing black hole attack in AODV through use of hash chain", in Proc. of 19th Iranian Conference Electrical Engineering (ICEE), Iran, pp. 1- 6, 2011.
[7] Yingbin Liang, H. Vincent Poor and Lei Ying "Secrecy Throughput of MANETs Under Passive and Active Attacks", IEEE transactions on information theory, vol. 57, no. 10, October 2011.
[8] Rajib Das," Security Measures for Black Hole Attack in MANET: An Approach", International Journal of Engineering Science and Technology (IJEST); Vol. 3, No. 4; 2011.
[9] Monita Wahengbam "Intrusion Detection in MANET using Fuzzy Logic", IEEE transactions on information theory,IEEE1884-1894, 2012.
[10] S.Sankara, Narayanan and Dr.S.Radhakrishnan "Secure AODV to Combat Black Hole Attack in MANET" International Conference on Recent Trends in Information Technology (ICRTIT), 2013.
[11] Mozmin Ahmed and Md. Anwar Hussain "Performance of an IDS in an Adhoc Network under Black Hole and Gray Hole attacks." International Conference on Electronics, Communication and Instrumentation (ICECI), 2014.
[12] Ravinder kaur, Jyoti kalra "Detection and prevention of black hole attack with digital signature" International Journal of Advanced Research in Computer Science and Software Engineering , ISSN: 2277 128, volume 4, issue 8, August 2014.
[13] Rashmi and Ameeta Seehra "A Novel Approach for Preventing Black-Hole Attack in MANETs" International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014.
[14] Yi, Ping, Zhoulin Dai, Shiyong Zhang, and Yiping Zhong. "A new routing attack in mobile ad hoc networks." International Journal of Information Technology 11, no. 2 (2005): 83-94.

[15] Li, Xiaoqing, et al. "An efficient anonymous routing protocol for mobile ad hoc networks." Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. Vol. 2. IEEE, 2009.
[16] Wu, Bing, Jianmin Chen, Jie Wu, and Mihaela Cardei. "A survey of attacks and countermeasures in mobile ad hoc networks." In Wireless Network Security,pp. 103-135. Springer US, 2007.
[17] Gagandeep, Aashima, and Pawan Kumar. "Analysis of different security attacks in MANETs on protocol stack a-review." International Journal of Engineering and Advanced Technology (IJEAT)1, no. 5 (2012): 2249.
[18] Abdelaziz, Amara Korba, Mehdi Nafaa, and Ghanemi Salim. "Survey of routing attacks and countermeasures in mobile ad hoc networks." In Computer Modelling and Simulation (UKSim), 2013 UKSim 15th International Conference on, pp. 693-698. IEEE, 2013.
[19] Capkun, Srdjan, Levente Buttya, and Jean-Pierre Hubaux. "Self-organized public-key management for mobile ad hoc networks." Mobile Computing, IEEE Transactions on2, no. 1 (2003): 52-64.
[20] Ahmad Anzaar, Husain Shahnawaz, Chand Mukesh, Dr SC Gupta, Dr R Gowri,H. L. Mandoria," Simulation Study for Performance Comparison of Routing Protocols In Mobile Adhoc Network",International Journal of World Academy Of Science Engineering and Technology (WASET),ICCSCN-2010 Singapore, issue no-70, pISSN 2010-376X, eISSN 2010-3778
[21] Singal, Gaurav, Harshit Garg, Vijay Laxmi, Manoj Singh Gaur, and Chhagan Lai. "Impact analysis of attacks in multicast routing algorithms in MANETs." In Industrial and Information Systems (ICIIS), 2014 9th International Conference on, pp. 1-6. IEEE, 2014.
[22] Medadian, Mehdi, Ahmad Mebadi, and Elham Shahri. "Combat with Black Hole attack in AODV routing protocol." In Communications (MICC), 2009 IEEE 9th Malaysia International Conference on, pp. 530-535. IEEE, 2009.
[23] Renu, Bahuguna, H.L. Mandoria and Tayal Pranavi. "Routing protocols in mobile ad-hoc network: a review." In Quality, Reliability, Security and Robustness in Heterogeneous Networks, pp. 52-60. Springer Berlin Heidelberg, 2013.
[24] Abusalah, Loay, Ashfaq Khokhar, and Mohsen Guizani. "A survey of secure mobile ad hoc routing protocols." Communications Surveys & Tutorials, IEEE 10, no. 4 (2008): 78-93.
[25] Madhusudhananagakumar, K. S., and G. Aghila. "A survey on Black Hole Attacks on AODV protocol in MANET." International Journal of Computer Applications (0975–8887) Volume (2011).
[26] Baadache, Abderrahmane, and Ali Belmehdi. "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." arXiv preprint arXiv:1002.1681 (2010).
[27] Tseng.Human-centric Computing and Information Sciences 2011 1:4 doi: 10.1186/2192-1962-1-4.
[28] Mukesh Chand and H.L. Mandoria "Merging independent mobile adhoc networks-A new methodology for autoconfiguration of IP addresses" International Journal of Engineering Science & Technology;Feb2013, Vol. 5 Issue 2, p20
[29] Sreenath, N., A. Amuthan, and P. Selvigirija. "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs." In Computer Communication and Informatics (ICCCI), 2012 International Conference on, pp. 1-7. IEEE, 2012.
[30] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of co-operative black hole attack in MANET." Journal of networks 3, no. 5 (2008): 13-20.